

**Commonwealth of Massachusetts
Information Technology Division**

**Enterprise Wireless Security Standards:
Wireless Local Area Networks
Version 1.1**

This document identifies standards to ensure secure deployment, use and administration of Wireless Local Area Networks (WLAN) by Commonwealth entities. Entities considering deployment of these technologies should first consult the Enterprise Wireless Security Policy. Entities covered by this policy must adhere to the standards detailed in this document for all WLAN deployments.

This document is one of the following Enterprise Wireless Security Standards documents that address major categories of wireless technology implementation:

- Wireless Local Area Networks (WLAN)
- Wireless Mobile Communications (WMC)
- Wireless Personal Area Networks (WPAN)
- Wireless Wide Area Networks (WWAN)

Additional references that entities may find useful as they plan WLAN deployments are listed at the end of this document.

Wireless Local Area Networks (WLAN)

802.11 Wireless LANs utilize unlicensed frequencies for communication between wireless clients and wireless access points (APs), which are usually connected to a wired network. Typical wireless LAN client devices include notebook and tablet computers and Personal Digital Assistants (PDAs) with 802.11 wireless network interface cards.

Commonwealth security standards for wireless LANs are based upon the industry standard *WiFi Protected Access*, also known by its acronym, WPA. The standard was proposed jointly by the IEEE and WiFi Alliance. WPA is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for WiFi networks. WPA has been designed to be forward compatible with the IEEE 802.11i specification. It utilizes enhanced data encryption through TKIP (Temporal Key Integrity Protocol) in addition to user authentication using 802.1X and EAP (Extensible Authentication Protocol).

1. Infrastructure Standards (WLAN)

A. Registration of access points

Commonwealth entities will assign specific responsibility for the creation and maintenance of a list identifying all WLAN access points.

B. Control of wireless spectrum/frequencies

Commonwealth entities will reserve the right to prohibit devices that may interfere with current and future wireless networks.

C. Physical Security of Access Points

Access points and cabling must be installed securely and lock-boxes are recommended where access points may be accessible to unauthorized staff or the public.

D. Prevention of rogue access points

Unregistered access points are prohibited and Commonwealth entities will configure and regularly monitor network to prevent installation of unregistered/unknown access points.

E. Separation of wireless and wired networks

Wireless Local Area Networks (WLANs) are vulnerable and must be treated like untrusted remote access networks rather than members of an internal (i.e., MAGNet) trusted network. As a result, a WLAN will be separated from wired network by an agency- or ITD-managed firewall; a WLAN will be installed using a physically separate wired network or as a VLAN on a shared wired/wireless infrastructure, separated by the firewall.

Please Note: Commonwealth entities must ensure that wireless users cannot bridge wired and wireless LANs by disabling default bridging capability in devices.

F. Management of Service Set Identifier (SSID)

Commonwealth entities will disable broadcast of access point SSIDs, and will develop the SSID naming convention (or adopt ITD's naming convention). The selected name(s) should not identify the Commonwealth entity or physical location of the network(s). In locations housing multiple Commonwealth entities, entities will cooperate on SSID naming conventions.

G. Disable connections 'across' access points

To increase management control and reduce risk of virus propagation across the wireless LAN, access points will be configured to prevent users connected to the same access point from communicating across the access point in peer-to-peer fashion (intra-Basic Service Set (BSS) relay).

H. Ensuring network availability, reliability and support

Commonwealth entities should develop policy-based network availability and reliability for high-priority traffic (e.g., for wireless mobile communication for emergency notification) requirements; Commonwealth entities or their network providers should establish requirements for Help Desk and support coverage (e.g., 24x7), maximum time to respond for service calls, service reliability (e.g., Mean Time Between Failures), network coverage, and maintenance of software and equipment at current firmware/software revision levels.

I. Monitor network security and performance

Commonwealth entities should effectively manage their wireless networks, including monitoring wireless network traffic, devices and potential security risks. Intrusion detection/prevention capability is recommended for networks. Commonwealth entities' network management practices must be documented.

2. Authentication & Encryption Standards (WLAN)

Commonwealth entities must confirm that all communications between wireless and wired networks include both user authentication and data encryption by using one of the methods identified in Section 2. "Authentication & Encryption Standards," and Section 3. "Device Configuration and Security Standards."

A. All wireless access points (AP's) and wireless network adaptors must employ one of the following security standards:

- WiFi Protected Access (WPA) standard utilizing 802.1x authentication, also called WPA enterprise. Use of WPA with pre-shared key (PSK) is prohibited;
- Robust Secure Network (RSN) standards that utilize both 802.1x extended authentication protocol and the advanced encryption standard (AES) specified within 801.11i;
- WiFi Protected Access 2 (WPA2) standard utilizing 802.1x authentication, also called WPA2 enterprise. Use of WPA2 with pre-shared key (PSK) is prohibited.

B. No unauthenticated access allowed on WAN/MAGNet

Unauthenticated public access is not allowed on the Commonwealth WAN or MAGNet network. Any WLAN that allows unauthenticated access must be separated from the WAN/MAGNet and treated as a separate DMZ external to the secure network; any access to the WAN/MAGNet from such a network must comply with the Commonwealth's [Enterprise Remote Access Security Policy](#) as published by ITD.

C. Encryption within applications required

Entities must be aware that outward facing applications (e.g., customer and vendor programs) may be running across insecure wireless networks at the customer or vendor site. Entities must design such applications to enforce data security through encryption at the application level (for example, SSL 128-bit encryption within browser for e-mail, or SSL web interface to customer facing systems). All such applications, whether for PC, PDA, SmartPhone, must support an Internet browser with a minimum SSL128-bit encryption (or equivalent for non-web applications).

D. Local caching, storing and printing

Entities must be aware that local storing, caching or printing of confidential data on remote devices may pose a significant data security risk. Entities must advise users that confidential data as defined by the entity cannot be stored on the devices unless strongly encrypted. Entities should develop a local policy as required to address this potential risk, in compliance with the Commonwealth's enterprise security policies as published by ITD, and relevant data confidentiality acts such as HIPAA, FIPA, or FERPA, based on the type of data involved.

E. Registration of devices

Entities must require registration of each wireless device prior to the device being admitted/connected to Commonwealth entities' LANs or WLANs. Serial numbers, phone numbers, MAC addresses, etc., as appropriate and obtainable for each wireless device, must be recorded. This information must be made available to ITD upon request.

3. Device Configuration and Security Standards (WLAN)

802.11 WLANs can inadvertently enable rapid propagation of viruses and other attacks, more so than properly configured wired networks. In addition, some WLAN installations allow "unknown" machines to participate in the network. The following standards must be followed to mitigate this risk:

A. Protection of connected devices

All devices that connect directly to the Commonwealth LAN/MAGNet via wireless networks must be configured in compliance with the Commonwealth's Enterprise security policies. Devices must be fully updated and patched, and must run personal firewall and anti-virus software, if available for the device, in compliance with Commonwealth and Commonwealth entities' policies.

B. Ownership of connected devices

All wireless communications devices that connect to the Commonwealth LAN/MAGNet must be the property of the Commonwealth. No personally owned wireless mobile communications devices or vendor equipment may be connected without express written permission of the Executive Department CIO, subsequent to a recommendation from the Enterprise Security Board. Entities may apply for variances to this ownership requirement on an application-specific basis.

All users of wireless communications devices must complete and sign a user acceptance agreement, similar to the current Virtual Private Network (VPN) user acknowledgement, allowing ITD and their Commonwealth entities to scan/monitor mobile communications devices during connection attempts to LAN/MAGNet resources and throughout the connected session. The user acknowledgement form must state that no one other than the authenticated user can use the device. Users of non-Commonwealth-owned devices who have been approved for such use must complete the same user agreement noted above.

C. Administrative control of connected devices

It is required that Commonwealth entities maintain exclusive administrative control of the configuration of all wireless devices directly connected to the LAN/MAGNet, to ensure that Spyware or sniffer software cannot be installed, the machine is free of viruses and the operating system is regularly updated.

D. No connection to non-Commonwealth entities' access points

No Commonwealth entities' wireless device may connect to wireless access points or networks external to the Commonwealth entities unless authorized by the Commonwealth entity. It is recommend that default Windows XP settings that connect to the access point with the strongest signal be reconfigured.

E. No ad hoc wireless networks

Commonwealth entities' 802.11 wireless devices may not connect directly to other Commonwealth entities' 802.11 wireless devices but instead must connect through the wireless access point and wired LAN. Entities must ensure that ad hoc network mode is disabled.

F. Physical security of remote devices

Entities must develop policies regarding physical security of remote devices, including procedures to prevent theft or loss, and to report theft or loss in the event of such occurrence. Entities and their network service providers should establish procedures and acceptable response times to terminate network access from lost or stolen devices. Commonwealth entities must advise users that confidential data, as defined by each Commonwealth entity, cannot be stored on remote devices.

Additional Reference

National Institute of Standards and Technology (NIST) Special Publication 800-48, "[Wireless Network Security: 802.11, Bluetooth and Handheld Devices](#)", by Tom Karygiannis and Les Owens, November 2002.

Cisco Systems White Paper, "[Security Architecture for the Enterprise \(SAFE\): Wireless LAN Security in Depth, Ver. 2](#)", by Sean Convery, Darrin Miller, Sri Sundaralingam, et al.